



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

February 12, 2019
Ref: FOIA-2015-00599

SENT ELECTRONICALLY TO: 17693-38969618@requests.muckrock.com

Mr. Shawn Musgrave
Muckrock
P.O. Box 55819
Boston, MA 02205-5819

Dear Mr. Musgrave:

This is in response to your Freedom of Information Act (FOIA) request for a copy of report DODIG-2015-117, Cyber Security U.S. Cyber Command and Military Services Need to Reassess Processes for fielding Cyber Mission Force Teams. We received your request on May 6, 2015, and assigned it case number FOIA-2015-00599.

The Office of the Deputy Inspector General for Audit conducted a search and found the enclosed record responsive to this request. After reviewing the record we determined that certain redacted portions are exempt from release pursuant to 5 U.S.C. § 552(b)(6), which pertains to information, the release of which would constitute a clearly unwarranted invasion of personal privacy and; 5 U.S.C. § 552 (b)(7)(E), which pertains to records or information compiled for law enforcement purposes, the release of which would disclose techniques and procedures for law enforcement investigations or prosecutions.

Additionally, in coordination with the Department of the Army, Department of the Navy, the United States Cyber Command, and the United States Marine Corps, other redacted portions are withheld from release in accordance with 5 U.S.C. § 552 (b)(1), which pertains to information that is currently and properly classified pursuant to Executive Order 13526, sections 1.4(a), and 1.4(g) and; 5 U.S.C. § 552 (b)(7)(E), as previously explained.

If you consider this to be an adverse determination, you may submit an appeal. Your appeal, if any, must be postmarked within 90 days of the date of this letter, clearly identify the determination that you would like to appeal, and reference the FOIA case number above. Send your appeal to the Department of Defense, Office of Inspector General, ATTN: FOIA Appellate Authority, Suite 10B24, 4800 Mark Center Drive, Alexandria, VA 22350-1500, or via facsimile to 571-372-7498. For more information on appellate matters and administrative appeal procedures, please refer to 32 C.F.R. Sec. 286.9(e) and 286.11(a).

February 12, 2019
Ref: FOIA-2015-00599

You may seek dispute resolution services and assistance with your request from the DoD OIG FOIA Public Liaison Officer at 703-604-9785, or the Office of Government Information Services (OGIS) at 877-684-6448, ogis@nara.gov, or <https://ogis.archives.gov/>. You may also contact OGIS via regular mail at National Archives and Records Administration Office of Government Information Services, 8601 Adelphi Road – OGIS, College Park, MD 20740-6001. Please note that OGIS mediates disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation.

If you have any questions regarding this matter, please contact the DoD OIG FOIA Requester Service Center at 703-604-9775 or via email at foiarequests@dodig.mil.

Sincerely,

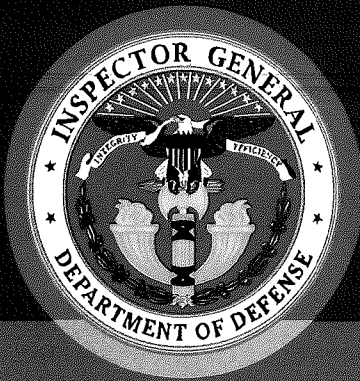
A handwritten signature in black ink, appearing to read "Mark Dorgan", with a long horizontal flourish extending to the right.

Mark Dorgan
Director
FOIA, Privacy and Civil Liberties Office

Enclosure(s):
As stated

SECRET//NOFORN

Project No. DODIG-2015-117



INSPECTOR GENERAL

U.S. Department of Defense

April 30, 2015



(U) U.S. Cyber Command and Military Services Need to Reassess Processes for Fielding Cyber Mission Force Teams

Classified By: Carol N. Gorman
Derived From: Multiple Sources
Declassify On: 20400430

Copy 23 of 38

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

SECRET//NOFORN

Released by DoD OIG FOIA in response to FOIA request # FOIA-2015-00590

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.



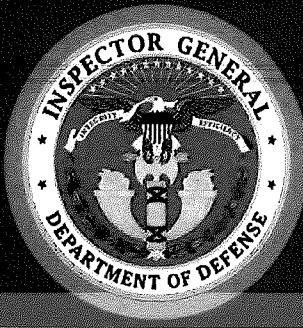
Fraud, Waste & Abuse

HOTLINE

Department of Defense

dodig.mil/hotline | 800 424 9098

For more information about whistleblower protection, please see the inside back cover.



Results in Brief

(U) U.S. Cyber Command and Military Services Need to Reassess Processes for Fielding Cyber Mission Force Teams

April 30, 2015

(U) Objective

(U) Our objective was to determine whether the U.S. Cyber Command (USCYBERCOM) and the Military Services effectively fielded Cyber Mission Force (CMF) teams.

(U) Finding

(S//REL TO USA, FVEY) USCYBERCOM and the Military Service cyber components did not effectively field CMF teams. Specifically, the Military Service cyber components did not declare ^{PER CY} of the required ^{PER CY} CMF teams ready for initial operational capability (IOC) by the end of FY 2014. This occurred because USCYBERCOM did not consider the level of effort needed to build the teams when it developed the CMF implementation plan. The Military Service cyber components also did not effectively plan for recruitment, retention, and training challenges associated with building a qualified workforce to support the CMF mission.

(S//REL TO USA, FVEY) In addition, we selected a non-statistical random sample of ^{PER CYBERCOM} CMF teams the Military Service cyber components projected or declared IOC by the end of FY 2014. We found that ^{PER CYBERCOM (b)} CMF teams sampled did not meet all IOC requirements. This occurred because the Military Service cyber components did not validate that the CMF teams met all IOC requirements before requesting IOC declaration from USCYBERCOM.

(U) Finding (cont'd)

(S//REL) Not meeting the requirements for IOC limits USCYBERCOM's ability to protect the DoD Information Network, support regional and functional commands, and defend our critical information and infrastructures.

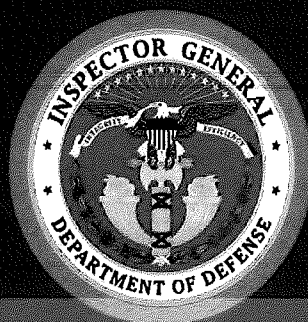
(U) Recommendations

(S) We recommend the Commander, U.S. Cyber Command, reevaluate and adjust the timeframes to allow the Military Service cyber components sufficient time to effectively field CMF teams. In addition, we recommend that the commanders at the Military Service cyber components:

- (S) develop strategies to ensure appropriate staffing of CMF teams and should consider the use of incentives, bonuses, and rotation extensions.
- (S) expand capability of existing training facilities and increase number and frequency of classes.
- (S) review internal processes used to declare CMF teams ready for IOC and implement procedures to ensure CMF teams meet all IOC requirements before IOC declarations are made.
- (S) validate CMF teams previously declared ready for IOC to ensure each team has core work roles assigned to appropriately trained personnel.

(U) Management Comments and Our Response

(S//NF) The Chief of Staff, USCYBERCOM, responding for the Commander, USCYBERCOM, partially addressed the recommendation stating that they had to apply pressure to the Services' manpower supply to address the significant and growing cyber threats. However, the Chief of Staff did not clarify whether he intends to adjust the fielding requirements to allow the Military Service cyber components sufficient time to field the remaining CMF teams. The Chief of Staff also disagreed with elements of the finding stating that the Department accepted the risks associated with rapidly growing the CMF to meet USCYBERCOM's urgent operational needs



Results in Brief

(U) U.S. Cyber Command and Military Services Need to Reassess Processes for Fielding Cyber Mission Force Teams

(S//NF) However, the timeframes for fielding CMF teams should be achievable and established in consideration of known constraints.

(S) Although the Commander, U.S. Army Cyber Command (ARCYBER), addressed the specifics of the recommendations, and no further comments are required, the Commander, disagreed with elements of the finding. The Commander stated PER US ARMY: (b) (1), 1.4(g)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(S//NF) Although the Commander, U.S. Fleet Cyber Command (FLTCYBER), did not respond to the recommendations, she provided comments that disagreed with elements of the finding. Specifically, the Commander disagreed that FLTCYBER PER US NAVY: (b) (1), 1.4(a), PER CYBERCOM (b) (1), 1.4(a)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(S//NF) We also revised page 7 of the report to reduce the number of CMF teams FLTCYBER would declare ready for IOC in FY 2015 from PER CYB CMF teams to PER CYB CMF team. In addition, the Commander, FLTCYBER, disagreed that

PER US NAVY: (b) (1), 1.4(a), PER CYBERCOM (b) (1), 1.4(a)

[REDACTED]

[REDACTED]

[REDACTED]

(U) The Commander, Air Forces Cyber, did not respond to the recommendations. Therefore, we request comments to the recommendations in the final report no later than May 29, 2015.

(S//NF) The Deputy Commander, Marine Corps Forces Cyberspace Command (MARFORCYBER), responding for the Commander, MARFORCYBER, disagreed with the recommendations and elements of the finding, stating MARFORCYBER developed a strategy for staffing CMF teams; offered recruiting and retention bonuses for Marines; PER USMC: (b) (1), 1.4(a)

[REDACTED]

[REDACTED]. Although the Deputy Commander stated MARFORCYBER extended rotations from PER USMC: (b) (1), 1.4(a), the Deputy Commander acknowledged that MARFORCYBER PER USMC: (b) (1), 1.4(a)

[REDACTED]

[REDACTED]

[REDACTED]. The Deputy Commander's statement conflicts with his comment to offer PER USMC: (b) (1), 1.4(a)

The Deputy Commander should clarify whether MARFORCYBER PER USMC: (b) (1), 1.4(a)

[REDACTED]

(U) Please see the Recommendations Table on the next page.

(U) Recommendations Table

Unclassified Management	Recommendations Requiring Comments	No additional Comments Required
(U) Commander, U.S. Cyber Command	1	
(U) Commander, U.S. Army Cyber Command		2, 4, and 5
(U) Commander, U.S. Fleet Cyber Command	3, 4, and 5	
(U) Commander, Air Forces Cyber	3, 4, and 5	
(U) Commander, Marine Corps Forces Cyberspace Command	2 and 3	4

(U) Please provide Management Comments by May 29, 2015.

April 30, 2015

MEMORANDUM FOR COMMANDER, U.S. CYBER COMMAND
COMMANDER, U.S. ARMY CYBER COMMAND
COMMANDER, U.S. FLEET CYBER COMMAND
COMMANDER, AIR FORCES CYBER
COMMANDER, MARINE CORPS FORCES CYBERSPACE COMMAND
ASSISTANT SECRETARY OF THE AIR FORCE (FINANCIAL
MANAGEMENT AND COMPTROLLER)
NAVAL INSPECTOR GENERAL
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: (U) U.S. Cyber Command and Military Services Need to Reassess
Processes for Fielding Cyber Mission Force Teams
(Report No. DODIG-2015-117)

~~(S//REL TO USA, FVEY)~~ We are providing this report for review and comment. U.S. Cyber Command and the Military Service cyber components did not effectively field Cyber Mission Force (CMF) teams. Specifically, the Military Service cyber components did not field ^{PER CY} of the ^{PER CY} CMF teams required to meet initial operational capability by the end of FY 2014. In addition, we selected a non-statistical random sample of ^{PER CYBERCOM} CMF teams the Military Service cyber components projected or declared IOC by the end of FY 2014, and found that ^{PER CYBERCOM (b) (1), 1.4(a)} CMF teams sampled did not meet all IOC requirements. We conducted this performance audit in accordance with generally accepted government auditing standards.

(U) We considered management comments on a draft of this report when preparing the final report. DoD Directive 7650.3 requires that recommendations be resolved promptly. Comments from the Commander, U.S. Army Cyber Command addressed the specifics of the recommendations, and no further comments are required. Comments from the Commander, U. S. Cyber Command, partially addressed Recommendation 1; therefore, we request additional comments. Comments from the Commander, Marine Corps Forces Cyberspace Command, partially addressed the recommendations; therefore, we request additional comments on Recommendations 2 and 3. The Commanders, U.S. Fleet Cyber Command and Air Forces Cyber, did not respond to the recommendations; therefore, we request that the Commanders provide comments on Recommendations 3, 4, and 5.

(U) Please send a portable document format (PDF) file containing your comments to ^{PER DOD OIG (b) (6)}. Copies of your comments must have the actual signature of the authorizing official for your organization. We cannot accept the /Signed/ symbol in place of the actual signature. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network (SIPRNET).

~~SECRET//NOFORN~~

(U) We should receive your comments by May 29, 2015. Comments provided on the final report must be marked and portion-marked, as appropriate, in accordance with DoD Manual 5200.01. If you consider any matters to be exempt from public release, you should mark them clearly for Inspector General consideration.

(U) We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 699-7331 (DSN 499-7331).



Carol N. Gorman
Assistant Inspector General
Readiness and Cyber Operations

~~SECRET//NOFORN~~

(U) Contents

(U) Introduction	1
(U) Objective	1
(U) Background	1
(U) Requirements for Cyber Mission Force Teams	3
(U) Review of Internal Controls	4
(U) Finding	5
(U) CMF Teams Not Effectively Fielded	5
(U) IOC Requirements Not Met	5
(U) Level of Effort to Field CMF Teams Not Fully Considered	7
(U) Military Service Cyber Components Faced Challenges	9
(U) CMF Teams Incorrectly Declared IOC	10
(U) Validation Procedures Did Not Exist	12
(U) Increased Risk of Adverse Impact on Cyber Resources	13
(U) Management Comments on the Finding and Our Response	13
(U) Recommendations, Management Comments, and Our Response	17
(U) Appendix A. (U) Scope and Methodology	24
(U) Use of Computer-Processed Data	26
(U) Use of Technical Assistance	26
(U) Prior Coverage	27
(U) Appendix B. CMF Staffing and Training Requirements	28
(U) Management Comments	33
(U) U.S. Cyber Command	33
(U) U.S. Army Cyber Command	36
(U) U.S. Fleet Cyber Command	39
(U) Marine Corps Forces Cyberspace Command	42
(U) Source of Classified Information	49
(U) Acronyms and Abbreviations	53

(U) Introduction

(U) Objective

(U) Our audit objective was to determine whether the U.S. Cyber Command (USCYBERCOM) and the Military Services effectively fielded Cyber Mission Force (CMF) teams. See Appendix A for a discussion of our scope and methodology and prior coverage.

(U) Background

(U) USCYBERCOM, a sub-unified command subordinate to U.S. Strategic Command, plans, coordinates, integrates, synchronizes, and conducts activities to:

- (U) direct the operations and defense of specified DoD information networks (DODIN);
- (U) prepare to conduct military cyberspace operations in all domains; and
- (U) ensure U.S. and Allied freedom of action in cyberspace and deny the same to our adversaries.

(S//NF) USCYBERCOM is also responsible for organizing and resourcing an appropriate cyberspace workforce to meet its three mission areas: defend the nation; support combatant command contingency and operational planning; and support the security, operation, and defense of the DODIN. To accomplish its mission, USCYBERCOM developed a Cyber Force Model in September 2012. The Secretary of Defense Deputy Management Action Group approved the Cyber Force Model in December 2012, with implementation to occur between FY 2013 and FY 2016. The model established the CMF, which includes:

- (U) National Mission Teams (NMTs) that defend the nation by executing offensive and defensive capabilities;
- (U) Combat Mission Teams (CMTs) that support combatant command contingency and operational planning;
- (U) Direct Support Teams (renamed National Support Teams [NSTs] and Combat Support Teams [CSTs]) that support the NMTs and CMTs; and
- (U) Cyber Protection Teams (CPTs) that defend the DODIN at the National, Combatant Command, and Military Service levels.

(U//~~FOUO~~) Collectively, the CMF is responsible for protecting key terrain and assets on all networks that comprise the DODIN.

(S//NF) In December 2012, USCYBERCOM recognized a significant deficiency existed in the number of cyber personnel that could support the Cyber Force Model. In addition, USCYBERCOM determined that the cyber workforce qualified to support the CMF consisted of ~~PER CYBER~~ personnel but a total of 6,187 were needed. To address the deficiency, USCYBERCOM tasked the Military Service cyber components¹ to build 133 CMF teams by the end of FY 2016. Table 1 shows that the greatest need for cyber personnel was for ~~PER CYBERCOM (b) (1), 1.4(a)~~ percent and ~~PER CY~~ percent of the total CMF teams needed, respectively.

(U) Table 1. Types of CMF Teams and Number of Personnel Needed by FY 2016

SECRET//REL TO USA, FVEY				
(U) Type of Team	(U) Number of Personnel per Team	(U) Number of Teams Needed	(U) Total Number of Personnel Needed	(U) Personnel by Team (percent)
(S//REL TO USA FVEY) NMT	PER CYBERCOM (b) (1), 1.4(a)			
(S//REL TO USA FVEY) NST				
(S//REL TO USA FVEY) CMT				
(S//REL TO USA FVEY) CST				
(S//REL TO USA FVEY) CPT				
(S//REL TO USA FVEY) Total		133	6,187	
SECRET//REL TO USA, FVEY				

¹ (U) The Military Service cyber components supporting the CMF effort include the U.S. Army Cyber Command, U.S. Fleet Cyber Command, Air Forces Cyber, and Marine Corps Forces Cyberspace Command.

(U) Requirements for Cyber Mission Force Teams

~~(S//REL TO USA, FVEY)~~ In FY 2013, USCYBERCOM issued two task orders (TASKORDs)² and one fragment order³ directing the Military Service cyber components to build a total of ~~PER~~^{PER}~~CY~~ CMF teams to initial operational capability (IOC) by the end of FY 2014.⁴ According to the TASKORDs, Military Service cyber components can declare CMF teams ready for IOC when each team possesses the ability and capacity to accomplish assigned missions and meet the following criteria:

- ~~(S//REL TO USA, FVEY)~~ fill a minimum of ~~PER~~^{PER}~~CY~~ percent of the core work roles, which differ by team. In addition, the individuals whose core work roles are included in the ~~PER~~^{PER}~~CY~~ percent must be fully trained and qualified. See Appendix B for a list of core work roles and training requirements by team.
- (U//~~FOUO~~) align each CMF team to its specific mission;
- (U//~~FOUO~~) allocate space that would allow personnel to perform duties, and ensure the teams have access to appropriate networks and data to accomplish assigned missions;
- (U//~~FOUO~~) place all available personnel in specific work roles that align with the mission;
- (U//~~FOUO~~) identify training requirements for all available team members; and
- (U//~~FOUO~~) ensure CSTs are aligned or identified for the build.

² ~~(S//REL TO USA, FVEY)~~ TASKORD 13-0244, "Establishment and Presentation of CMF Teams in FY 2013," March 6, 2013 and TASKORD 13-0747, "Establishment and Presentation of CMF Teams in FY 2014," October 11, 2013.

³ ~~(S//REL TO USA, FVEY)~~ Fragment Order-02 to USCYBERCOM TASKORD 13-0747 and Fragment Order-01, "Establishment and Presentation of CMF Teams in FY 2013," January 29, 2014.

⁴ ~~(S//REL TO USA, FVEY)~~ USCYBERCOM initially required that the Military Service cyber components build ~~PER~~^{PER}~~CY~~ CMF teams by the end of FY 2013. USCYBERCOM revised that requirement in January 2014, directing the Military Service cyber components to build all ~~PER~~^{PER}~~CY~~ teams by the end of FY 2014.

~~(S//REL TO USA, FVEY)~~ The FY 2014 IOC requirements for the Military Service cyber components were as follows.

- ~~(S//REL TO USA, FVEY)~~ U.S. Army Cyber Command (ARCYBER) – ~~PER~~^{PER}_{CY} teams
- ~~(S//REL TO USA, FVEY)~~ U.S. Fleet Cyber Command (FLTCYBER) – ~~PER~~^{PER}_{CY} teams
- ~~(S//REL TO USA, FVEY)~~ Air Forces Cyber (AFCYBER) – ~~PER~~^{PER}_{CY} teams
- ~~(S//REL TO USA, FVEY)~~ Marine Corps Forces Cyberspace Command (MARFORCYBER) – ~~P~~^P_E teams

(U) Review of Internal Controls

~~(S//REL TO USA, FVEY)~~ DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013, requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls. We identified internal control weaknesses related to USCYBERCOM and the Military Service cyber components' ability to effectively field CMF teams in a timely manner. Specifically, USCYBERCOM and the Military Service cyber components did not effectively field ~~PER~~^{PER}_{CYBERCOM} CMF teams by the end of FY 2014 and of the ~~PER~~^{PER}_{CY} CMF teams declared ready for IOC, ~~P~~^P_E did not meet all IOC requirements. We will provide a copy of this report to the senior officials responsible for internal controls in the CMF build.

(U) Finding

(U) CMF Teams Not Effectively Fielded

~~(S//REL TO USA, FVEY)~~ USCYBERCOM and the Military Service cyber components did not effectively field CMF teams. Specifically, the Military Service cyber components did not declare ~~PER CY~~ of the required ~~PER CY~~ CMF teams ready for IOC by the end of FY 2014. This occurred because USCYBERCOM did not consider the level of effort needed to build the teams when it developed the CMF requirements. The Military Service cyber components also did not effectively plan for recruitment, retention, and training challenges associated with building a qualified workforce to support the CMF mission.

~~(S//REL TO USA, FVEY)~~ In addition, we selected a non-statistical random sample of ~~PER CYBERCOM~~ CMF teams the Military Service cyber components projected or declared IOC by the end of FY 2014. We found that ~~PER CY~~ of the ~~PER CY~~ CMF teams sampled did not meet all IOC requirements. This occurred because senior officials at the Military Service cyber components did not validate that the CMF teams met all IOC requirements before requesting IOC declaration from USCYBERCOM.

~~(S//REL)~~ Not meeting the requirements for IOC limits USCYBERCOM's ability to protect the DODIN, support regional and functional commands, and defend our critical information and infrastructures.

(U) IOC Requirements Not Met

~~(S//REL TO USA, FVEY)~~ The Military Service cyber components did not declare ~~PER CY~~ of the required ~~PER CY~~ CMF teams ready for IOC by the end of FY 2014. Table 2 shows the progress of each Military Service cyber component in declaring CMF teams ready for IOC, with AFCYBER showing the least amount of progress in complying with the IOC requirements.

(U) Table 2. Status of CMF Teams by Military Service Cyber Component
(as of September 30, 2014)

SECRET//REL TO USA, FVEY				
(U) Military Service Cyber Component	(U) CMF Teams Required	(U) CMF Teams Fielded	(U) CMF Teams Not Fielded	(U) CMF Build Completion (percent)
(S//REL TO USA, FVEY) ARCYBER	PER CYBERCOM: (b) (1), 1.4(a); PER US NAVY: (b) (1), 1.4(a)			
(S//REL TO USA, FVEY) FLT CYBER				
(S//REL TO USA, FVEY) AFCYBER				
(S//REL TO USA, FVEY) MARFORCYBER				
(S//REL TO USA, FVEY) Total				
SECRET//REL TO USA, FVEY				

~~(S//REL TO USA, FVEY)~~ The Military Service cyber components developed a plan of action for declaring the remaining ~~PER CY~~ CMF teams ready for IOC as follows:

- ~~(S//REL TO USA, FVEY)~~ ~~PER CYBER~~ ARCYBER CMF teams by October 2014; ~~PER CYBE~~ CMF teams by December 2014;
- ~~(S//REL TO USA, FVEY)~~ ~~PER CYBER~~ FLT CYBER CMF teams by ~~PER US NAVY: (b) (1), 1.4(a); PER CYBERCOM~~
- ~~(S//REL TO USA, FVEY)~~ ~~PER CYBER~~ AFCYBER CMF teams by October 2014; ~~PER CYBER~~ CMF teams between November 2014 and April 2015; and
- ~~(S//REL TO USA, FVEY)~~ ~~PER CYBE~~ MARFORCYBER CMF team by March 2015.

~~(S//REL TO USA, FVEY)~~ As of December 19, 2014, the Military Service cyber components declared ~~PER CY~~ of those ~~PER CY~~ CMF teams ready for IOC. Specifically,

- ~~(S//REL TO USA, FVEY)~~ ARCYBER declared ~~PER CYBE~~ CMF teams ready for IOC in October 2014 and ~~PER CYBE~~ CMF teams ready for IOC in December 2014.
- ~~(S//REL TO USA, FVEY)~~ FLT CYBER declared ~~PER CYBERC~~ CMF teams ready for IOC ~~PER US NAVY: (b) (1), 1.4(a); PER CYBERCOM: (b) (1), 1.4(a)~~
- ~~(S//REL TO USA, FVEY)~~ AFCYBER declared ~~PER CYBE~~ CMF teams ready for IOC in October 2014 and ~~PER CYBERC~~ CMF teams ready for IOC in November 2014.

- ~~(S//REL TO USA, FVEY)~~ FLTCYBER – ~~PER~~ ~~CYBE~~ CMF team ~~PER US NAVY: (b)~~
~~(1), 1.4(a)~~
- ~~(S//REL TO USA, FVEY)~~ AFCYBER – ~~PER~~ ~~CYB~~ CMF teams between January 2015
and March 2015
- ~~(S//REL TO USA, FVEY)~~ MARFORCYBER – ~~PER~~ ~~CYBE~~ CMF team by March 2015

(S//REL TO USA, FVEY) USCYBERCOM did not properly consider the level of effort required to build the CMF teams when it developed the CMF requirements. When the USCYBERCOM Operations division initially issued the CMF requirements in March 2013, it did not include the training requirements and work roles. Four months later, in July 2013, USCYBERCOM established a training pipeline that listed the work roles and the training courses needed for each work role. This left 2 months for the Military Service cyber components to build PER CY CMF teams to IOC by September 30, 2013. According to USCYBERCOM senior officials, the plan was too aggressive to execute properly.

(S//REL TO USA, FVEY)
According to USCYBERCOM senior officials, the plan was too aggressive to execute properly.

~~(S//REL TO USA, FVEY)~~ Although USCYBERCOM extended the suspense date, the Military Service cyber components did not meet it. According to the Military Service cyber components, they did not meet their IOC requirements because of the need for Top Secret security clearances, lack of qualified and trained personnel, and lack of access to appropriate networks. Specifically,

- DODIG-2015-117 | 7

~~(S//REL TO USA, FVEY)~~ completing the background investigation portion of the security clearance process varied based on the personal circumstances of each candidate. It could also take up to an additional 8 months to clear a separate adjudication process.

- ~~(S//REL TO USA, FVEY)~~ FLTCYBER did not declare its ^{PER}_{CYBE} CMF teams ready for IOC because ^{PER}_{US NAVY: (b) (1), 1.4(a)}

^{PER}_{US NAVY: (b) (1), 1.4(a)} In addition, the JFHQ-C FLTCYBER Chief of Staff stated that ^{PER}_{US NAVY: (b) (1), 1.4(a)}

^{PER}_{US NAVY: (b) (1), 1.4(a)} The JFHQ-C FLTCYBER Chief of Staff explained that ^{PER}_{US NAVY: (b) (1), 1.4(a)}

^{PER}_{US}

- ~~(S//REL TO USA, FVEY)~~ AFCYBER personnel stated they could not declare their ^{PER}_{CYB} CMF teams ready for IOC because of a lack of training, personnel, and allocated workspace.
- ~~(S//REL TO USA, FVEY)~~ MARFORCYBER's Business Operations and Management Director stated MARFORCYBER could not declare ^{PER}_{CYBE} team ready for IOC because ^{PER}_{USMC: (b) (1), 1.4(a)}

^{PER}_{USMC: (b) (1), 1.4(a)} In addition, she stated USCYBERCOM did not establish the training requirements for ^{PER}_{USMC: (b) (1), 1.4(a)}

~~(S)~~ USCYBERCOM should reevaluate and adjust timeframes to allow the Military Service cyber components sufficient time to effectively field the ^{PER}_{CY} CMF teams and the remaining ^{PER}_{CY} CMF teams⁶ needed to meet the overall 133 CMF requirement.

⁵ ~~(S//REL TO USA, FVEY)~~ As of September 30, 2014, USCYBERCOM had not developed training requirements for Military Service CPTs.

⁶ ~~(S//REL TO USA, FVEY)~~ In addition to the ^{PER}_{CY} CMF teams the Military Service cyber components were to build by FY 2014, an additional ^{PER}_{CY} CMF teams are required to be built by FY 2016.

(U) Military Service Cyber Components Faced Challenges

(U) In addition to the level of effort required to declare CMF teams ready for IOC, the Military Service cyber components faced other challenges to building a qualified cyber workforce. Specifically,

- ~~(S//REL TO USA, FVEY)~~ recruiting efforts did not always attract personnel with the skills to perform cyber operations, personnel could not always obtain the appropriate security clearances, and retention efforts were not always effective; and
- ~~(S//REL TO USA, FVEY)~~ training courses were not always available, and ^{AR}
^{NI} [REDACTED]

(U) Recruiting and Retention Challenges

~~(S//REL TO USA, FVEY)~~ The Military Service cyber components' recruiting and retention efforts did not always attract or retain personnel with the skills to perform cyber operations. Specifically, the Military Service cyber components cited:

- ~~(S//REL TO USA, FVEY)~~ lack of interest in working for the Government because the private sector companies routinely offered more money at more attractive locations, and
- ~~(S//REL TO USA, FVEY)~~ military rotations and tour-of-duty lengths (the normal rotation was 2 years, and some work roles required 18 months of training).

~~(S//REL TO USA, FVEY)~~ In addition, the Military Service cyber components did not consistently offer recruitment and retention incentives such as enlistment and reenlistment bonuses, accelerated promotions, and referral bonuses. For example, although FLTCYBER ^{PER US NAVY: (b) (1), 1.4(a)} [REDACTED]

^{PER US NAVY: (b) (1), 1.4(a)} [REDACTED] MARFORCYBER ^{PER US NAVY: (b) (1), 1.4(a)} [REDACTED]

^{PER US NAVY: (b) (1), 1.4(a)} [REDACTED] In addition, only AFCYBER was developing a retention plan to retain CMF personnel for up to 8 years. ARCYBER did not implement a program that would offer any retention incentives. The Military Service cyber components should develop strategies to ensure appropriate staffing of CMF teams and should consider the use of incentives, bonuses, and rotation extensions.

(U) Limited Training Availability and ~~ARMY: (b)(7)(E)~~

~~(S//REL TO USA, FVEY)~~ Significant delays existed within the training pipeline that prevented the Military Service cyber components from effectively declaring CMF teams ready for IOC. For example, National Security Agency (NSA)-sponsored training courses were not always available to non-NSA team members on Military Service CPTs.

According to the JFHQ-C FLTCYBER Chief of Staff, ~~PER US NAVY: (b) (1), 1.4(a)~~

~~PER US NAVY: (b) (1), 1.4(a)~~ In

addition, the ARCYBER Branch Chief stated the aggressive training requirements created a demand for training that was greater than classroom capacity. Because each Military Service cyber component must send team members through the same courses, the training facilities were overwhelmed and unable to effectively accommodate

~~(S//REL TO USA, FVEY)~~
The JFHQ-C FLTCYBER Chief
of Staff also stated ~~PER US NAVY:
(b) (1), 1.4(a)~~

attendance requirements in a timely manner. The

JFHQ-C FLTCYBER Chief of Staff also stated ~~PER US NAVY: (b)
(1), 1.4(a)~~

According to the JFHQ-C FLTCYBER Chief of Staff and the MARFORCYBER Business Operations and Management Director, ~~PER US NAVY: (b) (1), 1.4(a)~~

~~PER US NAVY: (b) (1), 1.4(a)~~ However, there will continue to be a need for additional training courses. The Military Service cyber components should expand the capacity of the existing training facilities and increase the number of courses offered.

(U) CMF Teams Incorrectly Declared IOC

~~(S//REL TO USA, FVEY)~~ In addition to the ~~PER CY~~ CMF teams not declared ready for IOC by the end of FY 2014, we determined that ~~PER CYBERCOM
(b) (1), 1.4(a)~~ CMF teams declared ready for IOC did not meet all IOC requirements. We selected a non-statistical random sample of ~~PER CYBERCOM~~ CMF teams⁷ to evaluate the process used to declare teams ready for IOC. We reviewed the staffing and training status for the ~~PER CY~~ CMF teams to determine whether the Military Service cyber components complied with

~~(S//REL TO USA, FVEY)~~
~~ARMY:~~ team members were not
trained in accordance with
USCYBERCOM training
requirements

⁷ ~~(S//REL TO USA, FVEY)~~ The ~~PER~~ CMF teams represent the number of CMF teams the Military Service cyber projected or declared IOC by the end of FY 2014.

(U) Table 3. CMF Teams That Did Not Meet USCYBERCOM Training Requirement

⁸ (S//REL to USA, FVEY) MARFORCYBER CMF teams **PER CYBERCOM (b) (1)** met all IOC requirements.

(S//REL TO USA, FVEY) NAVY: (b)(1) 1.4(a)

[REDACTED]

[REDACTED]

[REDACTED]

(U) Table 4. CMF Teams That Did Not Assign Core Work Roles

SECRET//REL TO USA, FVEY		
(U) CMF Team	(U) Core Work Role Not Assigned	(U) Number Not Assigned
(U) FLTCYBER		
(S//REL TO USA, FVEY) PER CYBERCOM	PER CYBERCOM (b) (1), 1.4(a), PER US NAVY: (b) (1), 1.4(a)	
(S//REL TO USA, FVEY) PER CYBERCOM		
(S//REL TO USA, FVEY) PER CYBERCOM		
(S//REL TO USA, FVEY) Total FLTCYBER Work Roles Not Assigned		PER CYBERCOM (b) (1), 1.4(a), PER US
SECRET//REL TO USA, FVEY		

(U) Validation Procedures Did Not Exist

(S//REL TO USA, FVEY) Senior officials at the Military Service cyber components did not validate that the CMF teams met all IOC requirements before requesting IOC declaration from USCYBERCOM. Specifically, senior officials did not implement internal processes to verify that CMF team members were trained and CMF teams were staffed with core work roles. Instead, senior officials relied on parties responsible for staffing and training in support of the CMF plan to conclude teams were ready for IOC. Senior officials simply signed memorandums requesting USCYBERCOM declare teams ready for IOC. If senior officials had implemented a process for determining whether CMF teams met IOC requirements, they would have identified the PER CYBER CMF teams that did not meet those requirements. The results of testing only PER CYBERCOM CMF teams suggest there could be additional CMF teams that were declared ready for IOC without meeting the requirements for staffing and training. The Military Service cyber components should review the internal processes used to declare CMF teams ready

(S//REL TO USA, FVEY)
The results of testing only
PER CYBERCOM CMF teams suggest
there could be additional
CMF teams that were
declared ready for IOC
without meeting the
requirements for staffing
and training.

~~(S//REL TO USA, FVEY)~~ for IOC and implement procedures to ensure CMF teams meet all IOC requirements. In addition, the Military Service cyber components should validate CMF teams previously declared IOC to ensure each team has core work roles assigned to appropriately trained personnel.

(U) Increased Risk of Adverse Impact on Cyber Resources

~~(S//REL TO USA, FVEY)~~ Not meeting the requirements for IOC limits USCYBERCOM's ability to protect the DODIN, support regional and functional commands, and defend our critical infrastructures. According to the DoD Strategy for Operating in Cyberspace, DoD depends on cyberspace to perform its mission, operating over ~~PER CYBERCOM (b) (1), 1.4(a)~~ networks and ~~PER CYBERCOM (b) (1), 1.4(a)~~ computing devices around the globe. Countries such as ~~PER CYBERCOM (b) (1), 1.4(a)~~ work diligently to exploit DoD's unclassified and classified networks, which poses a significant threat to the health and safety of the warfighter and U.S. citizens. The cyber operations of these countries are increasing in number and sophistication. With the annual cost of global cyber crimes estimated at \$113 billion, it is necessary for DoD to maintain a robust cyber workforce that will work to reduce the impact and cost of cyber attacks and crimes.

(U) Management Comments on the Finding and Our Response

(U) U.S. Cyber Command Comments on the Finding

~~(S//NF)~~ The Chief of Staff, USCYBERCOM, responding for the Commander, USCYBERCOM, provided comments that disagreed with elements of the finding. Specifically, the Chief of Staff disagreed that USCYBERCOM did not consider the level of effort needed to build the CMF teams, stating that the Department accepted the risks associated with rapidly growing the CMF to meet USCYBERCOM's urgent operational need. According to the Chief of Staff, the Department stressed the traditional manning and training processes knowing that the urgency of need outpaced the Services' ability to staff and train the force. The Chief of Staff stated the management risks associated with rapidly building the CMF teams were discussed and documented in the Operations Deputies and Joint Chiefs of Staff Tank sessions during November-December 2012. This discussion occurred before the CMF teams were resourced by the Deputy Management

(S//NF) Action Group and codified in the Resource Management Decision signed by the Deputy Secretary of Defense. The Chief of Staff stated USCYBERCOM would continue to stress current Department processes and work with the Services to rapidly field CMF teams.

(U) Our Response

(S//NF) Comments from the Chief of Staff, USCYBERCOM, focused on the need to rapidly build the CMF teams and accepting the risks associated with establishing strict timeframes. We agree that an urgency exists and that USCYBERCOM accepted the associated risks with the aggressive timeframes. However, the timeframes should be achievable and established in consideration of known training constraints. For example, some work roles required 18 months of training and USCYBERCOM only allowed the Military Service cyber components one year to build CMF teams. As a result, Military Service cyber components could not achieve the required timeframes, even if stressing the Department's resources.

(U) Army Cyber Command Comments on the Finding

(S) Although the Commander, ARCYBER, provided comments that acknowledged challenges ARCYBER faced in building CMF teams, he disagreed that ARCYBER did not train ^{PER CY} team members. Specifically, the Commander stated he took responsibility for

PER US ARMY: (b) (1), 1.4(g)

. In addition, the Commander acknowledged that ARCYBER did not provide the audit team with up-to-date team rosters, training certificates, and transcripts; and supporting documentation. Furthermore, the Commander stated ^{PER US ARMY: (b) (1), 1.4(g)}

. The Commander also acknowledged that ARCYBER ^{PER US ARMY: (b) (1), 1.4(g)}

(U) Our Response

(S) Comments from the Commander, ARCYBER, focused on the support provided for IOC declarations. Although the Commander, ARCYBER, stated Table 3 incorrectly identified ^{PER CY} CMF team members as untrained, the audit team did not receive sufficient evidence supporting completed training. Specifically, ARCYBER provided rosters, training certificates, and transcripts that did not comply with USCYBERCOM

(S) requirements to have core work roles fully trained. In addition, ARCYBER did not provide supporting documentation to show USCYBERCOM

PER US ARMY: (b) (1),
1.4(e); PER CYBERCOM
(b) (1), 1.4(a)

(U) Fleet Cyber Command Comments on the Finding

(S//REL) The Commander, FLTCYBER, provided comments that disagreed with elements of the finding. Specifically, the Commander did not agree with the number of Navy CMF teams declared ready for IOC as of December 19, 2014 as stated in Table 2 of the report. The Commander stated FLTCYBER

PER US NAVY: (b) (1), 1.4(a); PER CYBERCOM (b) (1), 1.4(a)

According to the Commander, The Commander stated FLTCYBER

PER US NAVY: (b) (1), 1.4(a); PER CYBERCOM (b) (1), 1.4(a)

PER US NAVY: (b) (1), 1.4(a); PER CYBERCOM (b) (1), 1.4(a)

In addition, the Commander stated it

PER US NAVY: (b) (1), 1.4(a); PER CYBERCOM (b) (1), 1.4(a)

- (S//REL) FLTCYBER

PER US NAVY: (b) (1), 1.4(a); PER CYBERCOM (b) (1), 1.4(a)

- (S//NF)

PER US NAVY: (b) (1), 1.4(a); PER CYBERCOM (b) (1), 1.4(a)

(S//REL) Furthermore, the Commander stated that

PER US NAVY: (b) (1), 1.4(a); PER CYBERCOM (b) (1), 1.4(a)

According to the Commander,

PER US NAVY: (b) (1), 1.4(a); PER CYBERCOM (b) (1), 1.4(a)

The Commander also stated that

PER US NAVY: (b) (1), 1.4(a); PER
CYBERCOM (b) (1), 1.4(a)

(U) Our Response

(S//REL) Comments from the Commander, FLTCYBER, focused on

PER US NAVY: (b) (1), 1.4(a); PER
CYBERCOM (b) (1), 1.4(a)

(S//REL) As a result of the additional information from FLTCYBER, we updated page 6 of the report to [REDACTED]

PER US NAVY: (b) (1), 1.4(a), PER CYBERCOM: (b) (1), 1.4(a)

(U) Marine Corps Forces Cyberspace Command Comments on the Finding

(S) The Deputy Commander, MARFORCYBER, responding for the Commander, MARFORCYBER, provided comments that disagreed with elements of the finding. Specifically, the Deputy Commander stated that MARFORCYBER already developed a strategy to ensure appropriate staffing of CMF teams and established validation procedures to verify IOC declarations complied with USCYBERCOM IOC requirements. The Deputy Commander stated all levels of leadership reviewed the validity of the IOC declaration. In addition, the Deputy Commander stated the Services, not the cyber components, control the training facilities and are responsible for recruitment and retention. Also, the Deputy Commander stated that MARFORCYBER extended the tours of duty for Marines from [REDACTED]. According to the Deputy Commander, MARFORCYBER did not conduct an assessment to identify personnel with the aptitude for cyber operations.

PER US USMC: (b) (1), 1.4(a)

(U) Our Response

(S) Although the Deputy Commander, MARFORCYBER, stated MARFORCYBER had a strategy in place for appropriately staffing CMF teams, MARFORCYBER did not provide evidence of a strategy that ensured the CMF teams were fielded within the timeframes prescribed by USCYBERCOM. In addition, MARFORCYBER should be working with the Service headquarters to:

- (S) ensure training facilities can handle the increased attendance; and
- (S) obtain approval to offer potential cyber candidates recruiting and relocation incentives.

~~(S)~~ While the Deputy Commander stated MARFORCYBER did not conduct aptitude assessments, MARFORCYBER personnel informed the audit team, during discussions regarding recruitment, that MARFORCYBER did conduct assessments to identify personnel with the aptitude for cyber operations.

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation 1

~~(S)~~ We recommend the Commander, U.S. Cyber Command, reevaluate and adjust the timeframes to allow the Military Service cyber components sufficient time to effectively field Cyber Mission Force teams.

(U) U.S. Cyber Command Comments

~~(S//NF)~~ The Chief of Staff, USCYBERCOM, responding for the Commander, USCYBERCOM, partially agreed, stating that USCYBERCOM understood the desire to reevaluate the timeframes for effectively fielding CMF teams. However, the Chief of Staff stated that reevaluating the timeframes would not change the need to apply pressure to the Services' manpower supply to address the significant and growing cyber threat. The Chief of Staff also stated that ^{PER}~~CV~~ percent of the FY 2013 and FY 2014 teams reached IOC, and ^P~~E~~ percent of those teams achieved full operational capability. According to the Chief of Staff, if the Services were not pushed rapidly to build CMF teams, it would create an unacceptable military risk in defending the interests of the United States.

(U) Our Response

~~(S//NF)~~ Comments from the Chief of Staff did not address the recommendation. Although the Chief of Staff stated that ^{PER}~~CV~~ percent of the FY 2013 and FY 2014 CMF teams reached IOC, not all declarations complied with the timeframes and requirements established by USCYBERCOM. To meet the intent of our recommendation, the Commander, USCYBERCOM should reevaluate the current requirements and adjust the timeframes to be consistent with the training requirements for each CMF team. Although the Commander adjusted the requirements for fielding FY 2013 CMF teams, he did not adjust the timeframes for subsequent FYs. Accordingly, the Commander,

~~(S//NF)~~ USCYBERCOM should reconsider his decision to continue enforcing the requirements to rapidly declare CMF teams ready for IOC to allow Military Service cyber components sufficient time to effectively field the remaining CMF teams.

(U) Recommendation 2

~~(S)~~ We recommend the Commanders, U.S. Army Cyber Command and Marine Corps Forces Cyberspace Command, develop strategies to ensure appropriate staffing of CMF teams and should consider the use of incentives, bonuses, and rotation extensions.

(U) U.S. Army Cyber Command Comments

~~(S)~~ The Commander, ARCYBER, agreed, stating that the Army had retention incentives already in place for some military occupational specialties and approved additional retention incentives of Special Duty Assignment Pay and Assignment Incentive Pay in February 2015 for critical CMF occupational specialties. The Commander also stated that the Army prioritized the staffing of cyber units to expedite growth of highly trained cyber personnel for the CMF teams. In addition, the Commander stated by September 30, 2015, ARCYBER will implement the Operations Research and Systems Analysis to forecast the amount and timing of personnel needed to ensure future CMF teams reach IOC and full operational capability with the established milestones.

(U) Our Response

(U) Comments from the Commander, ARCYBER, addressed the specifics of the recommendation, and no further comments are required.

(U) Marine Corps Forces Cyberspace Command Comments

~~(S)~~ The Deputy Commander, MARFORCYBER, responding for the Commander, MARFORCYBER, disagreed, stating that MARFORCYBER developed a strategy that ~~PER USMC (b) (1), 1.4(a)~~. In addition, the Deputy Commander stated the Marine Corps offers recruiting and retention bonuses for Marines and recruiting, relocation, and retention incentives for Marine Corps civilian personnel. The Deputy Commander also stated that MARFORCYBER ~~PER USMC (b) (1), 1.4(a)~~

~~_____~~ However, the Deputy Commander stated perspective employees could request a hiring or relocation incentive.

(U) Our Response

~~(S)~~ Comments from the Deputy Commander, MARFORCYBER, did not address the specifics of the recommendation. Although the Deputy Commander stated MARFORCYBER ~~PER USMC (b) (1), 1.4(a)~~, the Deputy Commander acknowledged that MARFORCYBER ~~PER USMC (b) (1), 1.4(a)~~

~~PER USMC (b) (1), 1.4(a)~~. The Deputy Commander's statement conflicts with his comment to ~~PER USMC (b) (1), 1.4(a)~~. The Deputy Commander should clarify whether MARFORCYBER will implement ~~PER USMC (b) (1), 1.4(a)~~

(U) U.S. Cyber Command Comments

~~(U//FOUO)~~ Although not required to comment, the Chief of Staff, USCYBERCOM, disagreed, stating that the Services, not USCYBERCOM, are responsible for manning and training CMF team members. In addition, the Chief of Staff stated that the Services included the use of incentives, bonuses, and rotation extensions in their plans to staff the CMF teams.

(U) Our Response

~~(U//FOUO)~~ We acknowledge the comments from the Chief of Staff and agree that the Military Services cyber components are responsible for manning and training CMF team members. However, not all Military Service cyber components offered incentives, bonuses, or rotation extensions to attract qualified cyber personnel.

(U) Recommendation 3

~~(S)~~ We recommend the Commanders, U.S. Fleet Cyber Command, Air Forces Cyber, and Marine Corps Forces Cyberspace Command, expand the capability of existing training facilities and increase number and frequency of classes.

(U) Management Comments Required

(U) The Commanders, U.S. Fleet Cyber Command and Air Forces Cyber, did not respond to the recommendation. We request that the Commanders provide comments on the final report no later than May 29, 2015.

(U) Marine Corps Forces Cyberspace Command Comments

~~(S)~~ The Deputy Commander, MARFORCYBER, responding for the Commander, MARCORCYBER, disagreed, stating that increasing the size and the capability of service training facilities would not correct the current training deficiency. According to the Deputy Commander, the Marine Corps headquarters, not the cyber component, is responsible for training Marines while USCYBERCOM is responsible for training beyond the fundamentals provided by the Marine Corps. In addition, the Deputy Commander stated the specialized training is provided by the National Security Agency's Associate Director for Education and Training.

(U) Our Response

~~(S)~~ The Deputy Commander, MARFORCYBER, did not address the specifics of the recommendation. To meet the intent of the recommendation, MARFORCYBER should coordinate with Marine Corps headquarters, USCYBERCOM, and the National Security Agency, to develop training expansion plans that would ensure the capacity of training facilities adequately accommodate CMF team members. This would ensure CMF team members receive required training in a timely manner. Accordingly, the Commander, MARFORCYBER needs to clarify whether MARFORCYBER will develop a plan, in conjunction with the Service headquarters, to expand training facility capacity to meet the training requirements established by USCYBERCOM. In addition, although the Deputy Commander stated USCYBERCOM is responsible for training beyond the Marine Corps' fundamental training, USCYBERCOM only provides funding for CMF training and does not offer training courses.

(U) U.S. Cyber Command Comments

~~(U//FOUO)~~ Although not required to comment, the Chief of Staff, USCYBERCOM, disagreed, stating that USCYBERCOM provided initial training for the 2013 surge capacity while the Services ramped up their manning and training processes. According to the Chief of Staff, AFCYBER worked with the U.S. Air Force to complete a course resource estimate to double training capacity for select initial and intermediate Air Force cyber courses in calendar year 2015.

(U) Our Response

(U//~~FOUO~~) We acknowledge the comments from USCYBERCOM and agree that the Military Service cyber components are responsible for expanding the capability of existing training facilities and increasing the number and frequency of classes. However, not all Military Service cyber components expanded the training capacity to ensure that required cyber training was available to CMF team members when needed.

(U) Recommendation 4

~~(S)~~ We recommend the Commanders, U.S. Army Cyber Command, U.S. Fleet Cyber Command, Air Forces Cyber, and Marine Corps Forces Cyberspace Command, review internal processes used to declare Cyber Mission Force teams ready for initial operational capability and implement procedures to ensure Cyber Mission Force teams meet all initial operational capability requirements before issuing initial operational capability declarations.

(U) Management Comments Required

(U) The Commanders, U.S. Fleet Cyber Command and Air Forces Cyber, did not respond to the recommendation. We request that the Commanders provide comments on the final report no later than May 29, 2015.

(U) U.S. Army Cyber Command Comments

~~(S)~~ The Commander, ARCYBER, agreed, stating ARCYBER would continue to improve its existing processes for tracking the completion of required training. In addition, the Commander stated ARCYBER would update procedures for declaring CMF teams ready for IOC immediately to include requirements to:

- ~~(S)~~ perform audits and inspections of the equivalency records;
- ~~(S)~~ verify ARCYBER rosters with the USCYBERCOM digital battle rosters;
- ~~(S)~~ ensure that appropriate waivers are obtained in writing; and
- ~~(S)~~ document the risk assumed by the Commander in the IOC memoranda to USCYBERCOM.

(U) Our Response

(U) Comments from the Commander, ARCYBER, addressed all specifics of the recommendation, and no further comments are required.

(U) Marine Corps Forces Cyberspace Command Comments

~~(S)~~ The Deputy Commander, MARFORCYBER, responding for the Commander, MARFORCYBER, disagreed, stating MARFORCYBER had procedures in place for reviewing internal processes for declaring CMF teams ready for IOC. Specifically, the Commander stated that leaders at all levels monitored training processes and validated the progress of CMF teams to ensure IOC declarations met USCYBERCOM requirements.

(U) Our Response

(U) Although the Deputy Commander, MARFORCYBER, stated internal processes existed, MARFORCYBER personnel did not describe procedures for validating IOC compliance. If implemented as described in MARFORCYBER's comments, the process should improve MARFORCYBER's ability to meet USCYBERCOM CMF requirements. As a result, comments from the Deputy Commander, MARFORCYBER, addressed all specifics of the recommendation, and no further comments are required.

(U) U.S. Cyber Command Comments

(U//~~FOUO~~) Although not required to comment, the Chief of Staff, USCYBERCOM, agreed with the recommendation. According to the Chief of Staff, all service cyber components instituted a review process to ensure CMF teams declared ready for IOC satisfy the USCYBERCOM IOC criteria. In addition, the Chief of Staff stated that waivers are fully documented and USCYBERCOM implemented a verification process for IOC declarations.

(U) Our Response

(U//~~FOUO~~) We acknowledge the comments from USCYBERCOM. However, not all Military Service cyber components provided evidence of implementing processes for ensuring CMF teams met all IOC requirements before issuing IOC declarations.

(U) Recommendation 5

(S) We recommend the Commanders, U.S. Army Cyber Command, U.S. Fleet Cyber Command, and Air Forces Cyber, validate Cyber Mission Force teams previously declared ready for initial operational capability to ensure each team has core work roles assigned to appropriately trained personnel.

(U) Management Comments Required

(U) The Commanders, U.S. Fleet Cyber Command and Air Forces Cyber, did not respond to the recommendation. We request that the Commanders provide comments on the final report no later than May 29, 2015.

(U) U.S. Army Cyber Command Comments

(S) The Commander, ARCYBER, agreed, stating that ARCYBER will conduct a comprehensive review of the CMF teams previously declared IOC by performing audits and inspections over the course of the next year. In addition, the Commander stated ARCYBER would report material deficiencies to USCYBERCOM no later than March 1, 2016.

(U) Our Response

(S) Comments from the Commander ARCYBER addressed all specifics of the recommendation, and no further comments are required.

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this performance audit from May 2014 through February 2015, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

~~(S//REL TO USA, FVEY)~~ We interviewed personnel from USCYBERCOM, ARCYBER, FLTCYBER, AFCYBER, and MARFORCYBER. We also reviewed the following USCYBERCOM guidance to determine whether USCYBERCOM and the Military Service cyber components appropriately declared teams ready for IOC.

- ~~(S//REL TO USA, FVEY)~~ USCYBERCOM TASKORD 13-0244, "Establishment and Presentation of CMF Teams in FY 2013," March 6, 2013;
- ~~(S//REL TO USA, AUS, CAN, GDR, NZL)~~ USCYBERCOM TASKORD 13-0747, "Establishment and Presentation of CMF Teams in FY 2014," October 11, 2013;
- ~~(S//REL TO USA, FVEY)~~ Fragment Order-02 to USCYBERCOM TASKORD 13-0747, "Establishment and Presentation of CMF Teams in FY 2014," January 29, 2014;
- (U//~~FOUO~~) "CMF Training Pipeline," Version 1.1, July 17, 2013; and
- (U//~~FOUO~~) "CMF Training Pipeline," Version 2.2, June 18, 2014.

(U) We focused on the following requirements of the USCYBERCOM TASKORDs to verify whether the Military Service cyber components effectively fielded CMF teams. The CMF teams needed to have:

- ~~(S//REL TO USA, FVEY)~~ ^{PER CY} percent of the team assigned, to include a core number of personnel in specified work roles;
- ~~(S//REL TO USA, FVEY)~~ a sub-set of those core personnel who were trained and qualified. See Appendix B for details on the specific team members in core work roles who must be assigned and trained;

- (U//~~FOUO~~) the CMF team's mission alignment process completed; and
- (U//~~FOUO~~) space allocated for personnel in work roles to perform duties with appropriate access to networks and data to accomplish assigned missions.

(S//~~REL TO USA, FVEY~~) We selected a non-statistical random sample of ^{PER CYBERCOM} CMF teams¹ to evaluate the process used to declare the teams ready for IOC. We ensured the sample of teams included a representation of the different types of CMF teams across each Military Service.

(S//~~REL TO USA, FVEY~~) For the ^{PER CY} CMF teams, we requested battle rosters, training records, and evidence of mission alignment and space allocation. Table A-1 shows the number of CMF teams USCYBERCOM required each Military Service cyber component to build by the end of FY 2014.

(U) Table A-1. Required Number of CMF Teams by the end of FY 2014

SECRET//REL TO USA, FVEY	
(U) Military Service Cyber Component	(U) Number of CMF Teams Required
(S// REL TO USA, FVEY) ARCYBER	^{PER CYBERCOM (b) (1), 1.4(a)}
(S// REL TO USA, FVEY) FLTCYBER	
(S// REL TO USA, FVEY) AFCYBER	
(S// REL TO USA, FVEY) MARFORCYBER	
(S// REL TO USA, FVEY) Total	
SECRET//REL TO USA, FVEY	

(S//~~REL TO USA, FVEY~~) Table A-2 identifies the CMF teams sampled per Military Service cyber component.

¹ (S//~~REL TO USA, FVEY~~) The ^{PER} CMF teams represent the number of CMF teams the Military Service cyber components reported were ready for IOC or projected to be ready for IOC by the end of FY 2014.

(U) Table A-2. Sample of CMF Teams Selected

UNCLASSIFIED// FOR OFFICIAL USE ONLY		
(U) Service	(U) Team ID	(U) Team Type
1. ARCYBER	PER DOD OIG (b) (7)(E), PER US ARMY (b) (7)(E)	
2. ARCYBER		
3. ARCYBER		
4. ARCYBER		
5. ARCYBER		
6. FLTCYBER		
7. FLTCYBER		
8. FLTCYBER		
9. FLTCYBER		
10. FLTCYBER		
11. AFCYBER		
12. AFCYBER		
13. AFCYBER		
14. AFCYBER		
15. MARFORCYBER		
16. MARFORCYBER		
UNCLASSIFIED// FOR OFFICIAL USE ONLY		

(U) Use of Computer-Processed Data

(U) We used computer-processed data from the Enterprise Learning Management system. The system is a data repository the Military Service cyber components used to manage, track, and report training activities. To obtain reasonable assurance of the data's reliability, we compared completion certificates to the training transcripts to confirm that training records were accurate. As a result, we concluded that the data provided as evidence of training completion was reliable.

(U) Use of Technical Assistance

(U) The Quantitative Methods Division provided assistance during the audit. The Quantitative Methods Division assisted with the non-statistical sampling methodology for selecting CMF teams to test compliance with USCYBERCOM's fielding requirement.

(U) Prior Coverage

(U) During the last 5 years, the Government Accountability Office (GAO) and the Department of Defense Inspector General (DoD IG) issued three reports related to DoD cyber activities. Unrestricted GAO reports can be accessed at <http://www.gao.gov>. DoD IG reports can be accessed at <http://www.dodig.mil/pubs/index.cfm>.

(U) GAO

(U) Report No. GAO-11-75, "Defense Department Cyber Efforts: DoD Faces Challenges in its Cyber Activities," July 25, 2011

(U) Report No. GAO-11-421, "Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities," May 20, 2011

(U) DoD OIG

(U//~~FOUO~~) Report No. DODIG-2015-048, "Joint Cyber Centers PER DOD OIG (b) (7)(E)
[REDACTED] Cyberspace Operations," December 9, 2014

(U) Appendix B

(U) CMF Staffing and Training Requirements

~~(S//REL TO USA, FVEY)~~ Each type of CMF team had different staffing and training requirements. To meet the IOC requirements, each CMF team needed to be at least ~~PER CYB~~ percent staffed and the staff had to fill specific core work roles. In addition, some or all of the staff in the core work roles had to be trained and qualified for the position.

(U) NMT Staffing and Training Requirement

~~(S//REL TO USA, FVEY)~~ According to TASKORD 13-0747, each NMT will have a staff of ~~PER CYB~~. To meet IOC requirements, the NMT needed to be staffed and trained as shown in Table B-1.

(U) Table B-1. NMT Staffing and Training Requirement

SECRET//REL TO USA, FVEY		
(U) Core Work Role	(U) Number of Personnel Required	(U) Number of Personnel Required to be Trained
<div>PER CYBERCOM (b) (1), 1-4(a)</div> <div></div>		
SECRET//REL TO USA, FVEY		

(U) CMT Staffing and Training Requirement

~~(S//REL TO USA, FVEY)~~ According to TASKORD 13-0747, each CMT will have a staff of ^{PER}_{CYB}. To meet IOC requirements, the CMT needed to be staffed and trained as shown in Table B-3.

(U) Table B-3. CMT Staffing and Training Requirement

SECRET//REL TO USA, FVEY		
(U) Core Work Role	(U) Number of Personnel Required	(U) Number of Personnel Required to be Trained
PER CYBERCOM (b) (1), 1.4(a)		
<div></div>		
SECRET//REL TO USA, FVEY		

(U) CST Staffing and Training Requirement

~~(S//REL TO USA, FVEY)~~ According to TASKORD 13-0747, each CST will have a staff of ^{PER}_{CYB} To meet IOC requirements, the CST needed to be staffed and trained as shown in Table B-4.

(U) Table B-4. CST Staffing and Training Requirement

SECRET//REL TO USA, FVEY		
(U) Core Work Role	(U) Number of Personnel Required	(U) Number of Personnel Required to be Trained
PER CYBERCOM (b) (1), 1-4(a)		
<div></div>		
SECRET//REL TO USA, FVEY		

(S//REL TO USA, FVEY) According to TASKORD 13-0747, each CPT will have a staff of PER
CYB. To meet IOC requirements, the CPT needed to be staffed and trained as shown in Table B-5.

(U) Table B-5. CPT Staffing and Training Requirement

SECRET//REL TO USA, FVEY		
(U) Core Work Role	(U) Number of Personnel Required	(U) Number of Personnel Required to be Trained
<p>PER CYBERCOM (b) (1), 1.4(a)</p>		
<p>SECRET//REL TO USA, FVEY</p>		

~~SECRET//NOFORN~~

Management Comments

(U) Management Comments

(U) U.S. Cyber Command

~~SECRET//NOFORN~~



DEPARTMENT OF DEFENSE
UNITED STATES CYBER COMMAND
9800 SAVAGE ROAD, SUITE 6477
FORT GEORGE G. MEADE, MARYLAND 20755

13 Mar 2015

Reply to:
Chief of Staff

MEMORANDUM FOR THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

Through: VICE CHAIRMAN, JOINT CHIEFS OF STAFF

Subject: (U) U.S. Cyber Command and Military Services Need to Reassess Processes for
Fielding Cyber Mission Force Teams (Draft Report for Project No. D2014-D000RC-
0179)

1. ~~(S//REL TO USA, FVEY)~~ United States Cyber Command (USCYBERCOM) appreciates the opportunity to respond to the subject Department of Defense Inspector General (DoDIG) report. USCYBERCOM non-concurs with the finding that USCYBERCOM did not consider the level of effort needed to build the teams and two of the four recommendations. The two recommendations in question require USCYBERCOM's components to develop strategies to ensure appropriate staffing of Cyber Mission Force (CMF) teams (including use of incentives, bonuses, and rotation extensions) and expand capability of existing training facilities and number and frequency of classes, but cites USCYBERCOM as being responsible for organizing and resourcing the cyber workforce.

2. ~~(U//FOUO)~~ The Services, not USCYBERCOM, are statutorily required to man and train the force, as defined in 10 U.S.C. and implemented through Department of Defense Directive 5100.01. As such, the Services, as part of their common military service functions, received the resources (e.g., billets and funding) to staff the CMF. Consistent with their statutory authority, each Service developed plans to man the CMF teams. The Services' plans include any appropriate uses of incentives, bonuses, and rotation extensions required to establish and sustain the force. For example, the U.S. Air Force instituted Selective Reenlistment Bonus Programs for ~~PER CYBERCOM (b) (1), 1.4(a)~~ work roles on 5 Dec 2013. Consequently, the Services have completed the two recommended actions.

3. ~~(U//FOUO)~~ The portion of the recommendation for USCYBERCOM to expand capability of existing training facilities and increase the number and frequency is completed. As explained to the audit team, USCYBERCOM, within the scope of its authorities, provided initial training surge capacity in 2013, while the Services ramped up their manning and training processes

Classified By ~~PER DOD~~
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20370801

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(U) U.S. Cyber Command (cont'd)

~~SECRET//NOFORN~~

accordingly. USCYBERCOM completed this action in direct response to the known level of effort needed to train CMF personnel based on the Services' manning projections to field the CMF, according to the phasing and resources approved by the Deputy Secretary of Defense via the Deputy's Management Action Group (DMAG). This provided time for the Services to plan and start expanding their training capabilities.

4. ~~(S//NF)~~ For example, Air Forces Cyber (AFCYBER), working with U.S. Air Force (USAF), completed an Air Force Course Resource Estimate for expanded training capacity that was approved and resourced in FY14 for implementation in calendar year 2015. The changes will effectively double classroom capacity for both Initial and Intermediate Air Force cyber training courses for ~~PER CYBERCOM (b) (1), 1.4(a)~~ career fields. AFCYBER has also coordinated with the Air Staff and Air Education and Training Command to expand recruitment and technical training pipelines to meet the ~~PER CYBERCOM (b) (1),~~ needs of the CMF. As a result, the ~~PER CYBERCOM (b) (1), 1.4(a)~~ at Goodfellow Air Force Base have expanded their throughput to match CMF requirements. Furthermore, the USAF has more than doubled their Joint Cyber Analysis Course throughput from 96 seats in 2012 (pre-CMF) to 196 in 2014, and requirements are continually being re-evaluated by CMF planners and training managers.

5. ~~(S//NF)~~ The general finding that USCYBERCOM and Military Service cyber components did not effectively field CMF teams is consistent with the known challenges the Department expected to face when standing up the new CMF. This is mainly because the Department, in a fully coordinated response to the threat, accepted the risk to rapidly grow the CMF in order to meet USCYBERCOM's urgent operational need, knowing the urgency of need outpaced the Services' diverse manning and training processes. As substantiated by the Chairman, Joint Chiefs of Staff (JCS), in his Action Memo signed by the Secretary of Defense (SECDEF) on 11 Dec 2012, the Department needed to move aggressively to stand up the CMF in order to address the cyber threat. The subject report should include this fact, which provides context for subsequent actions.

6. ~~(U//FOUO)~~ Moving aggressively required the Department to knowingly stress traditional manning and training processes built prior to the advent of the cyber domain. These traditional processes lack the agility and flexibility required to keep pace with the ever-changing cyber threat. The management risks associated with the need to rapidly build the CMF were discussed and documented in the Operations Deputies and JCS TANK sessions during the November-December 2012 timeframe, before the CMF was resourced by the DMAG as codified in the Resource Management Decision signed by the Deputy SECDEF. The report should address these key events where the level of effort to build the CMF was discussed, courses of actions considered, and the phased build approach was developed. The report also should account for the intervening Joint Staff (JS) actions with the Services that occurred during the September-December 2012 timeframe.

7. ~~(S//NF)~~ Although USCYBERCOM understands the management desire to reevaluate timeframes to effectively field CMF teams, it will not change the operational imperative or need to pressurize the Services' manpower supply systems to have teams in place immediately in order to address the significant and growing threat. Without stipulating the requirements for when specific operational capabilities were needed, the Department would not be where it is

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

9. (U) My point of contact for this action is [REDACTED] PER DOD OIG: (b) (6)

(U) U.S. Army Cyber Command



~~SECRET~~
DEPARTMENT OF THE ARMY
U.S. ARMY CYBER COMMAND AND SECOND ARMY
8825 BEULAH STREET
FORT BELVOIR, VIRGINIA 22060-5246

ARCC-IR

06 MAR 2015

MEMORANDUM FOR

Department of Defense (DoD) Inspector General (IG), ATTN: PER DOD OIG (b) (6)
Program Director, Readiness and Cyber Operations, 4800 Mark Center Drive,
Alexandria, Virginia 22350
US Cyber Command (USCC), ATTN: PER DOD OIG (b) (6) J8, Capabilities and
Resources, 9800 Savage Road, PER DOD OIG (b) (7)(F) Fort Meade, MD 20755

SUBJECT: Command Comments to DoDIG Draft Report: U.S. Cyber Command and
Military Services Need to Reassess Process for Fielding Cyber Mission Force Teams
(D2014-D000RC-0179.000) dated 13 February 2015 (U)

1. (U) US Army Cyber Command has reviewed the subject draft report and concurs with the recommendations. Enclosed are our comments to recommendations 2, 4, and 5 of the above report.
2. (U) The remaining recommendations did not require a response from us.
3. (U) In addition, we have general comments on the report as a whole, some of which are regarding the specific facts you used to support your findings. Those comments follow our responses to the recommendations.

4. (U) If you have any questions, please contact PER DOD OIG (b) (6)
PER DOD OIG (b) (6)

(b) (6)

Encl

CF:
HQDA (DAMO-ODCI)
HQDA (SAAG-ACFO)

CLASSIFIED BY: PER DOD OIG (b) (6)
DERIVED FROM: USCCI 5200-07, 1.4(a)
DECLASSIFY ON: 20250227

~~SECRET~~
This document is UNCLASSIFIED
When separated from classified enclosure

(U) U.S. Army Cyber Command (cont'd)~~SECRET~~

DOD IG DRAFT REPORT DATED 13 FEBRUARY 2015
DOD IG PROJECT NO D2014-D000RC-0179.000

**"U.S. CYBER COMMAND AND MILITARY SERVICES NEED TO REASSESS PROCESSES
FOR FIELDING CYBER MISSION FORCE (CMF) TEAMS"**

**ARMY CYBER COMMAND COMMENTS
TO THE DOD IG RECOMMENDATIONS**

(C) RECOMMENDATION 2: DoD IG recommends the Commanders, U.S. Army Cyber Command and Marine Corps Forces Cyberspace Command, develop strategies to ensure appropriate staffing of CMF teams and should consider the use of incentives, bonuses, and rotation extensions.

(C) ARMY CYBER RESPONSE: Concur. The Army had existing retention incentives already in place for some Military Occupational Specialties (MOSs) critical to the CMF Team build. In February 2015, HQDA approved additional retention incentives of Special Duty Assignment Pay (SDAP) and Assignment Incentive Pay (AIP) to critical CMF MOSs. Additionally, the Army prioritized the fill of cyber units to expedite growth of highly trained CMF cyber warriors. Going forward, ARCYBER is implementing Operations Research and Systems Analysis (ORSA) support to provide quantitative and accurate forecasting to the U.S. Army Human Resources Command (HRC). These forecasts will better articulate the amount and timing of personnel needed to ensure future teams reach Initial Operational Capability (IOC) and Full Operational Capacity (FOC) within forecasted build goals. This analytical model capability will be available NLT 30 September 2015.

(C) RECOMMENDATION 4: DoD IG recommends the Commanders, U.S. Army Cyber Command, Air Forces Cyber, and Marine Corps Forces Cyberspace Command, review internal processes used to declare Cyber Mission Force teams ready for initial operational capability and implement procedures to ensure Cyber Mission Force teams meet all initial operational capability requirements before issuing initial operational capability declarations.

(C) ARMY CYBER RESPONSE: Concur. The Army continues to improve existing processes for tracking completion of required training that influences IOC/FOC declarations. Publication of US Cyber Command (USCC) Fragmentary Order (FRAGO) 6 to Task Order (TASKORD) 13-0747 in the next 30 days will refine the IOC/FOC process. Immediately, ARCYBER will update its IOC declaration procedures to include verifying the training or training equivalency of team members by auditing/inspecting the training records, verifying rosters with USCC's digital Battle Roster, obtaining any waivers in writing, and documenting risk assumed by the commander in IOC memoranda to USCC. This process will be implemented immediately.

(C) RECOMMENDATION 5: DoD IG recommends the Commanders, U.S. Army Cyber Command, U.S. Fleet Cyber Command, and Air Forces Cyber, validate Cyber Mission Force teams previously declared ready for initial operational capability to ensure each team has core work roles assigned to appropriately trained personnel.

(C) ARMY CYBER RESPONSE: Concur. Army Cyber Command will conduct a comprehensive review of teams previously declared IOC using audits and inspections over the

~~SECRET~~

(U) U.S. Army Cyber Command (cont'd)

~~SECRET~~

course of the next year. We will complete the review no later than 1 March 2016 and will report any material deficiencies to USCC as they occur.

~~(U//FOUO)~~ **FURTHER COMMENTS ON THE REPORT AS A WHOLE:** In addition to these recommendations provided by the DOD IG, Army Cyber Command has the following comments with respect to the report:

(U) ~~PER US ARMY: (b) (7)(E)~~

~~(U)~~ ~~PER US ARMY: (b) (1), 1.4(g)~~

(U) In summary, on page 11 Table 3, it was incorrect to state that ~~PER~~ Army team members were not trained in accordance with USCYBERCOM training requirements. More specifically,

- ~~PER CYBERCOM (b)~~ personnel were trained at the time the team was declared IOC; however, the system of record was in error, or the certificates and transcripts reflected different names for the same courses (e.g. transcript read "Network +" but requirement was for NETW1050). ~~PER CYBERCOM (b) (1), 1.4(g)~~
- ~~PER CYBERCOM (b) (1), 1.4(g)~~ personnel had a waiver or equivalency for a single course; however, we lacked supporting documentation at the time the team was declared IOC. ~~PER CYBERCOM (b) (1), 1.4(g)~~ immediately, written documentation will be retained to support all waivers and course equivalency credit prior to IOC declaration.
- ~~PER CYBERCOM (b) (1), 1.4(g)~~ remaining personnel were not required for the team to be declared IOC. DoD IG requested documentation for them based on outdated rosters. ~~PER CYBERCOM (b) (1), 1.4(g)~~ immediately, documentation retention will be reviewed to ensure an audit trail of rosters and subsequent updates exist.
- The remaining ~~PER~~ in their final course at the time of IOC declaration; the command was advised that ~~PER US ARMY: (b) (1), 1.4(g)~~ ~~PER CYBERCOM (b) (1), 1.4(g)~~ In the future, any risk assumed by the commander will be documented on the declaration memo.

We will continue to refine processes and procedures for the efficient build of effective CMF teams.

~~SECRET~~

(U) U.S. Fleet Cyber Command

Final Report
Reference



~~SECRET//REL EXEMPT, AUC, CAN, CDR, NZL~~
DEPARTMENT OF THE NAVY
COMMANDER U.S. FLEET CYBER COMMAND
9800 SAVAHL ROAD, Suite 6506
Fort George G. Meade, MD 20755-6506

3000
Ser N00/S104
13 Mar 15

MEMORANDUM

From: Commander, U.S. Fleet Cyber Command/U.S. TENTH Fleet
To: Department of Defense Inspector General

Subj: U.S. FLEET CYBER COMMAND RESPONSE TO DOD IG FINAL
DRAFT REPORT OF 13 FEBRUARY 2015 (U)

Ref: (a) Draft Report DoD IG Project No. D2014-D000RC-
0179.000, "U.S. Cyber Command and Military Services
Need to Reassess Processes for Fielding Cyber
Mission Force Teams (S//REL)

Encl: (1) Recommended Changes to Reference (a)
(2) ~~PER~~ ~~CVR~~ National Mission Team Initial Operational
Capability Declaration (S//REL)
(3) ~~PER~~ ~~CVR~~ Cyber Protection Team (CPT) Initial Operational
Capability (IOC) Declaration (S//REL)
(4) ~~PER~~ ~~CVR~~ Cyber Protection Team Initial Operational
Capability Declaration (S//REL)
(5) ~~PER~~ ~~CVR~~ Cyber Mission Team (CMT) Initial Operational
Capability (IOC) Declaration (S//REL)

1. (U) Thank you for the opportunity to provide a response to
reference (a). Recommended changes are detailed in enclosure
(1) with supporting documentation provided by enclosures (2)
through (5).

2. (U) My POC is ~~PER~~ ~~DOD~~ ~~OIG~~ (b) (6)
~~PER~~ ~~DOD~~ ~~OIG~~ (b) (6)

(b) (6)

Copy to:
USCYBERCOM

~~SECRET//REL EXEMPT, AUC, CAN, CDR, NZL~~

Omitted
declaration memos
for CMF teams ~~PER~~
~~CY~~
because of length.
Copies provided
upon request.

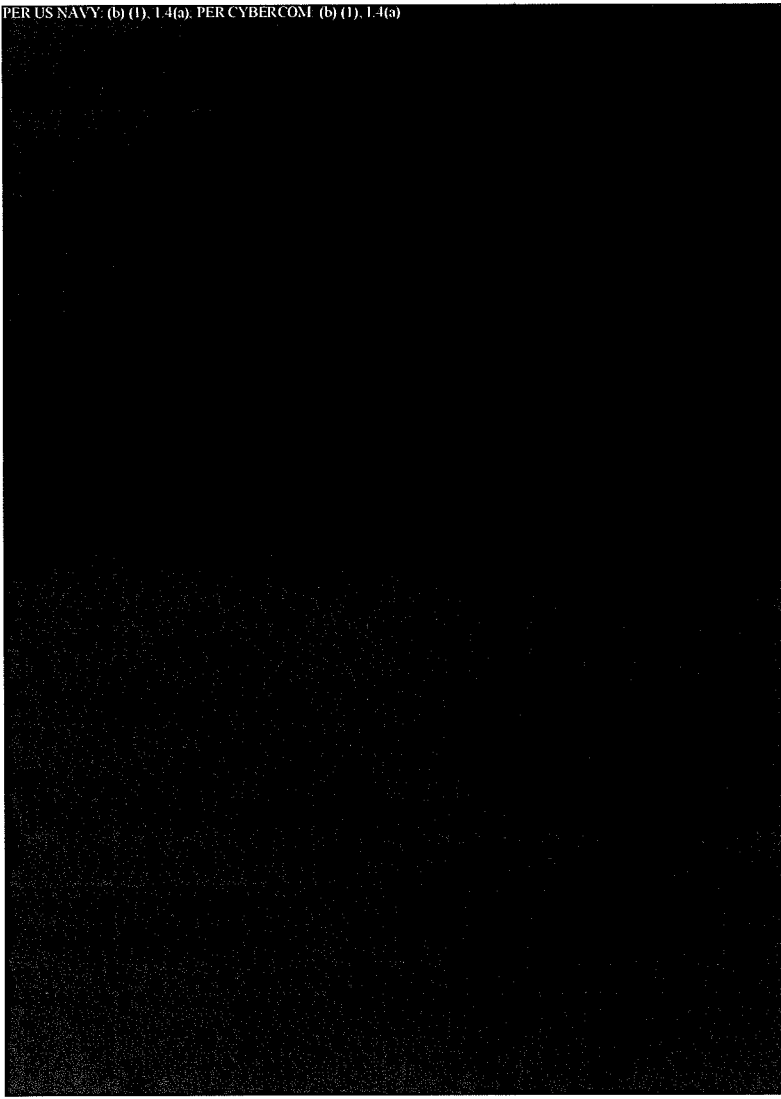
(U) U.S. Fleet Cyber Command (cont'd)

Final Report
Reference

~~SECRET//NOFORN~~

Recommended changes to reference (a)

PER US NAVY (b) (1), 1.4(a), PER CYBERCOM (b) (1), 1.4(a)



Revised

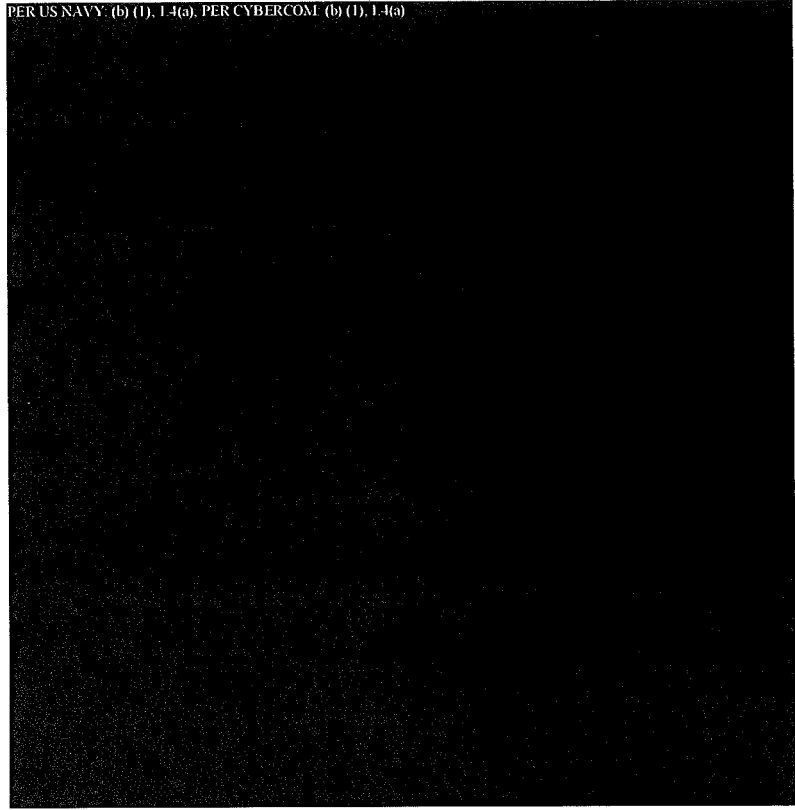
Revised

Enclosure (1)

~~SECRET//NOFORN~~

(U) U.S. Fleet Cyber Command (cont'd)

~~SECRET//NOFORN~~
PER US NAVY (b) (1), 1.4(a), PER CYBERCOM (b) (1), 1.4(a)



(U) Marine Corps Forces Cyberspace Command



UNITED STATES MARINE CORPS
U.S. MARINE CORPS FORCES CYBERSPACE COMMAND
8800 SAVAGE ROAD, SUITE 6850
FORT GEORGE G. MEADE, MD 20755-6000

ADRES REFER TO
5041
RMD

MAR 16 2015

From: Commander, U.S. Marine Corps Forces Cyberspace Command
To: Distribution List

Subj: Draft Report for Project No. D2014-D000RC-0179.000, "U.S. Cyber Command and Military Services Need to Reassess Processes for Fielding Cyber Mission Force Teams," dated February 13, 2015

Encl: DoD IG CRM ~~(S//NF)~~

1. **PURPOSE.** To transmit the approved MARFORCYBER comments pertaining to the Draft Report for Project No. D2014-D000RC-0179.000.

2. **BACKGROUND.** (U//~~FOUO~~) The Office of the Inspector General, Department of Defense, issued the draft report for Project No. D2014-D000RC-0179.000, "U.S. Cyber Command and Military Services Need to Reassess Processes for Fielding Cyber Mission Force Teams," dated February 13, 2015 for MARFORCYBER review and comment. Instructions are for MARFORCYBER to provide comments on whether management agrees or disagrees with the finding and recommendations in the report. If in agreement, MARFORCYBER is instructed to describe what actions have been taken or planned to accomplish the recommendations including the completion dates. If in disagreement, MARFORCYBER is instructed to give specific reasons of disagreement and propose alternative action if appropriate.

3. **DISCUSSION.** MARFORCYBER disagrees with the draft report as written and has (7) critical, (6) substantive, and (1) administrative comments with respect to the subject task (see classified Enclosure (1) for our Comment Resolution Matrix).

A. Recommendation 1. Not applicable to MARFORCYBER.

B. Recommendation 2. HQMC is offering the Marine (0689's) a recruiting/retention bonus. As for Civilian Marines, M&PA authorizes appropriate compensation tools to include the 3 R's - Recruiting, Relocation and Retention Incentives on an as needed and justified basis in accordance with Department of Navy Civilian Human Resource policy. Salary is negotiable only for new federal employees. Existing federal employees follow standard salary/promotion policies as established by the Office of Personnel Management.

C. Recommendation 3. See Enclosure (1).

D. Recommendation 4. See Enclosure (1).

E. Recommendation 5. Not applicable to MARFORCYBER.

(U) Marine Corps Forces Cyberspace Command (cont'd)

4. VIEW OF OTHERS. MARFORCYBER Approving official: PER DOD OIG (b) (6)
PER DOD OIG (b) (6) Deputy Commander, MARFORCYBER.

5. The point of contact for this memorandum is the PER DOD OIG (b) (6)
PER DOD OIG (b) (6)

PER DOD OIG (b) (6)

Deputy Commander

Copy to:
DoD IG
USCYBERCOM J-8
File

(U) Marine Corps Forces Cyberspace Command (cont'd)

SECRET//NOFORN							COMMENT	RATIONALE	DECISION (If any)
ITEM	#	SOURCE	TYPE	PAGE	PARA	LINE			
1	1	MFCY	EC	1	5	3 & 4	199 In addition, we recommend that the commanders at the Military Service cyber components consider the following as appropriate:	199 Consistency. The recommendation is incongruent with the report's findings and recommendations listed at the closing. Sub bullet "a" recommends that the United States Marine Corps (USMC) Per USMC (b)(1) Sec 1.4(a)	
2	2	MFCY	EC	4	2	3-4	200-202 (b)(1) (b)(2) (b)(3) This occurred because senior officials at some of the Military Service cyber components did not validate that the CMC teams met all IOC requirements before requesting IOC declaration from USCYBERCOM	(Disputed) Accuracy. MAHFORCYBER established procedures to validate CMC teams met USCYBERCOM's requirements. The IG audit found	

Page 3 of 8

(U) Marine Corps Forces Cyberspace Command (cont'd)

Final Report
Reference

SECRET//NOFORN							COMMENT	RATIONALE	DECISION (EC/SA)
ITEM	#	SOURCE	TYPE	PAGE	PARA	LINE			
3.	3	MFCY	EC	8	4	1-5	SECRET//NOFORN MARFORCYBER's Business and Operations and Management Director stated MARFORCYBER personnel stated that they could not declare [REDACTED] specific team IOC because this team [REDACTED] PER USMC (b) (1) 1.4(a) [REDACTED] In addition, she stated that USCYBERCOM did not establish the training requirements for [REDACTED] [REDACTED] was unable to meet the USCYBERCOM IOC work role training requirements.	no discrepancies when looking at USMC teams (acknowledged in foot note 7 on page 11). Accuracy and consistency. Recommend MARFORCYBER Per USMC (b)(1) Sec. 1-4(a)	
4.	4	MFCY	EC	10	1	19-21	SECRET//NOFORN The Military Service Cyber Components. USCYBERCOM should expand the capacity of the existing training facilities and increase the number of courses offered	(U) Accuracy. USCYBERCOM is responsible for budgeting and providing training which is non MOS specific. ADET and contractors currently provide most of the CMF training. Furthermore, the services, not the cyber components control the training facilities.	
5.	5	MFCY	EC	12	2	1	SECRET//NOFORN Senior officials at a number of the Military Service cyber components did not validate that the CMF teams met all IOC requirements before requesting IOC declaration from USCYBERCOM. Per USMC (b)(1) Sec. 1-4(a) [REDACTED]	(U) Accuracy. The training and validation program of MARFORCYBER's team IOC was reviewed at all leadership levels. Consequently, the IG inspectors found no deviations when they conducted a review of MARFORCYBER's CMF teams.	
6.	6	MFCY	EC	13	5	1-3	SECRET//NOFORN We recommend the Commanders, U.S. Fleet Cyber Command, Air Forces Cyber, and Marine Corps Forces Cyberspace Command, expand the capability of existing training facilities and increase number and frequency of classes. USCYBERCOM continue to review CMI training requirements, service provided training, specialized training, and increase both the number and frequency of specialized	Consistency and accuracy. Per USMC (b)(1) Sec. 1-4(a)	

Page 4 of 8

Page 19

(U) Marine Corps Forces Cyberspace Command (cont'd)

Final Report
Reference

SECRET//NOFORN							COMMENT	RATIONALE	DECISION (EC/2/3)
ITEM	#	SOURCE	TYPE	PAGE	PARA	LINE			
							training classes as required.	Per USMIC (b)(1) Sec. 1-4(a)	
7.	7	MFCY	EC	14	1	2-3	464 We recommend the Commanders, U.S. Army Cyber Command, U.S. Fleet Cyber Command and Air Forces Cyber, and Marine Corps Forces Cyberspace Command, review internal processes used to declare Cyber Mission Force teams ready for initial operational capability and implement procedures to ensure Cyber Mission Force teams meet all initial operational capability requirements before issuing initial operational capability declarations.	464 Accuracy. MARFORCYBER Per USMIC (b)(1) Sec. 1-4(a)	
8.	8	MFCY	S	5	1	4-8	464 SECRET//NOFORN This occurred because USCYBERCOM did not consider the level of effort needed to build the teams when it developed the CMF requirements. USCYBERCOM did not provide the military services with planning information to field CMF forces in a timely enough manner so that the services could effectively plan for the associated. The Military Service cyber components also did not effectively plan for recruitment, retention, and training challenges associated with building a qualified workforce to support the CMF mission.	464 SECRET//NOFORN Accuracy. The added information underscores the variety of initial issues the military services experienced in providing CMF forces in a timely manner. Additionally, the military services, not the cyber components are responsible for recruitment, retention and MOS training.	
9.	9	MFCY	S	9	2	7-9	464 SECRET//NOFORN Per USMIC (b)(1) 1-4(a)	464 Accuracy. The current wording suggests that Per USMIC (b)(1) Sec. 1-4(a)	

Page 19

Page 21

Page 5 of 8

(U) Marine Corps Forces Cyberspace Command (cont'd)

SECRET//NOFORN							COMMENT	RATIONALE	DECISION (EC/SA)
ITEM	#	SOURCE	TYPE	PAGE	PARA	LINE			
10.	10	MFCY	S	9	3	5-6	<p>SECRET//NOFORN... For example, although FLICYBER PER USMC (b) (1), 1-4(a) PER USMC (b) (1), 1-4(a)</p>	<p>IG inspection report and took corrective action. CME members serve a PER USMC (b) (1), 1-4(a)</p> <p>(U) Accuracy and consistency. Personnel recruitment is a complicated process. The current wording in the paragraph links PER USMC (b) (1), 1-4(a) PER USMC (b) (1), 1-4(a). However, both programs are related to different HR policies and guidance. In the interest of cost savings and funding shortfalls, MARFORCYBER PER USMC (b) (1), 1-4(a)</p> <p>Per USMC (b)(1) Sec. 1-4(a)</p>	
11.	11	MFCY	S	9	3	8-10	<p>SECRET//NOFORN... The Military Service cyber components should further develop strategies to ensure appropriate staffing of CMF teams and should consider the use of incentives, bonuses, and rotation extensions as required."</p>	<p>(U) Accuracy. The USMC has a recruitment and training strategy which is always being reviewed to meet USMC and other requirements. The current wording suggests components have no strategy. Furthermore, meeting USCYBERCOM required specialized training requirements has been delayed by an overstated ADET training program. ADET increased output at time allowed.</p>	
12	12	MFCY	S	10	1	16-18	<p>SECRET//NOFORN... Although FLICYBER and MARFORCYBER began conducting assessments to identify personnel with the aptitude for cyber operations, which PER USMC (b)(1) Sec. 1-4(a)</p>	<p>(U) Accuracy. MARFORCYBER has not conducted such an assessment. MARFORCYBER is aware of an</p>	

Page 6 of 8

(U) Marine Corps Forces Cyberspace Command (cont'd)

SECRET//NOFORN							COMMENT		RATIONALE	DECISION (EC/SA)
ITEM	#	SOURCE	TYPE	PAGE	PARA	LINE				
							need for additional training courses		effort by University of Maryland Center of Advanced Study of Language to develop an cyber aptitude assessment process. However, this initiative is in its infancy and MARFORCYBER has not participated.	
13.	13	MFCY	S	13	4	1-3	444 We recommend the Commanders, U.S. Army Cyber Command and U.S. Marine Corps Forces Cyberspace Command, develop continuing <u>to improve</u> strategies to ensure appropriate staffing of CMF teams and should consider the use of incentives, bonuses, and retention extensions.		444 Accuracy. The current wording inaccurately implies that MARFORCYBER has no strategy to meet USCYBERCOM's CMF build goals. MARFORCYBER met PER of the IOC build requirements highlighted in the report. MARFORCYBER has developed a strategy to include PER for all of our cyber team members. Additionally, Headquarters Marine Corps is currently offering the Marine (0689's) a recruiting retention bonus. Lastly, MARFORCYBER offers Recruiting, Relocation and Retention Incentives to civilian Marines in accordance with M&RA policies.	
14.	14	MFCY	A	11	Foot-note 7		444 REL to USA, EYB MARFORCYBER MARFORCYBER CMF teams PER CYBERCOM met all IOC requirements.		(U) Accuracy. Misspelling	

Page 18

Revised

(U) Source of Classified Information

(U) The documents listed below are sources used to support information within this report.

- Source 1: (U) USCYBERCOM - Cyber Threat Brief
Classified By: ~~PER DOD OIG (b) (6)~~
Derived from: USCYBERCOM Security Classification Guide, date 20111011 and Derived from: National Security Agency/Central Security Service Policy Manual 1-52; dated: 20070108
Declassify on: 20380701
- Source 2: (U) USCYBERCOM Cyber Mission Force Model
Classified By: ~~PER DOD OIG (b) (6)~~
Derived from: USCYBERCOM Security Classification Guide; dated: 20111011 and Derived from: National Security Agency/Central Security Service Policy Manual 1-52; dated: 20070108
Declassify on: 20380514
- Source 3: (U) Cost Assessment and Program Evaluation Cyber Issue Team Deputy Management Action Group Comeback
Classified by: Multiple Sources
Declassify on: 20330831
- Source 4: (U) Cyber Force Concept of Operations & Employment, Annex D
Classified By: ~~PER DOD OIG (b) (6)~~
Derived from: USCYBERCOM Security Classification Guide; dated: 20111011 and Derived from: National Security Agency/Central Security Service Policy Manual 1-52; dated: 20121116
Declassify on: 20381120

- Source 5: (U) Cyber Force Concept of Operations & Employment, Annex E
Classified By: ~~PER DOD OIG: (b) (6)~~
Derived from: USCYBERCOM Security Classification Guide;
dated: 20111011 and Derived from: National Security
Agency/Central Security Service Policy Manual 1-52;
dated: 20121116
Declassify on: 20381120
- Source 6: (U) Cyber Force Concept of Operations & Employment, Annex H
Classified By: ~~PER DOD OIG: (b) (6)~~
Derived from: USCYBERCOM Security Classification Guide;
dated: 20111011 and Derived from: National Security
Agency/Central Security Service Policy Manual 1-52;
dated: 20121116
Declassify on: 20381120
- Source 7: (U) ~~PER DOD OIG: (b) (7)(E)~~ Initial Operational Capability
Declaration Memorandum, Classified By: ~~PER DOD OIG: (b) (6)~~
Derived from National Security Agency/Central Security Service
Policy Manual 1-52; Dated: 20070108
Declassify on: 20390101
- Source 8: (U) ~~PER DOD OIG: (b) (7)(E)~~ Initial Operational Capability
Declaration Memorandum, Classified By: ~~PER DOD OIG: (b) (6)~~
Derived from National Security Agency/Central Security Service
Policy Manual 1-52; dated: 20070108
Declassify on: 20381201
- Source 9: (U) ~~PER DOD OIG: (b) (7)(E)~~ Initial Operational Capability
Declaration Memorandum
Derived from National Security Agency/Central Security Service
Policy Manual 1-52; Dated: 20070108
Declassify on: 20390101

- Source 10: (U) ~~PER DOD OIG. (b) (7)(E)~~ Battle Roster
Derived from: National Security Agency/Central Security Service
Policy Manual 1-52; dated: 20070108
Declassify on: 20390901
- Source 11: (U) ~~PER DOD OIG. (b) (7)(E)~~ Battle Roster
Derived from: National Security Agency/Central Security Service
Policy Manual 1-52; dated: 20070108
Declassify on: 20390901
- Source 12: (U) MARFORCYBER, Cyber Mission Force Team Review
Derived from: National Security Agency/Central Security Service
Policy Manual 1-52; dated: 20070108
Declassify on: 20390901
- Source 13: (U) ~~PER DOD OIG. (b) (7)(E)~~ Initial Operational Capability
Declaration Memorandum, Derived from: National Security
Agency/Central Security Service Policy Manual 1-52
Declassify on: 20390801
- Source 14: (U) ~~PER DOD OIG. (b) (7)(E)~~ Initial Operational Capability
Declaration Memorandum, Derived from: National Security
Agency/Central Security Service Policy Manual 1-52
Declassify on: 20390801
- Source 15: (U) ~~PER DOD OIG. (b) (7)(E)~~ Initial Operational Capability
Declaration Memorandum, Derived from: National Security
Agency/Central Security Service Policy Manual 1-52
Declassify on: 20390801
- Source 16: (U) ARCYBER Cyber Mission Force Overview
Derived from: National Security Agency/Central Security Service
Policy Manual 1-52
Declassify on: 20390701

- Source 17: (U) ^{PER DOD OIG (b) (7)(E)} Initial Operational Capability
Declaration Memorandum

Derived from National Security Agency/Central Security Service
Policy Manual 1-52; Dated: 20070108

Declassify on: 20390101
- Source 18: (U) FLTCYBER Cyber Mission Force Team Overview

Derived from National Security Agency/Central Security Service
Policy Manual 1-52; Dated: 20070108

Declassify on: 20390101
- Source 19: (U) ^{PER DOD OIG (b) (7)(E)} Initial Operational Capability
Declaration Memorandum

Derived from National Security Agency/Central Security Service
Policy Manual 1-52; Dated: 20070108

Declassify on: 20390101
- Source 20: (U) Combat Protection Team Support to Defend US Strategic
Command Critical Mission Systems

Derived from National Security Agency/Central Security Service
Policy Manual 1-52; Dated: 20070108

Declassify on: 20390101
- Source 21: (U) ARCYBER Mission Brief

Derived from National Security Agency/Central Security Service
Policy Manual 1-52; Dated: 20070108

Declassify on: 20390101

(U) Acronyms and Abbreviations

AFCYBER	Air Forces Cyber
ARCYBER	U.S. Army Cyber Command
CMF	Cyber Mission Force
CMT	Combat Mission Team
CPT	Cyber Protection Team
CST	Combat Support Team
DODIN	DoD Information Network
FLTCYBER	U.S. Fleet Cyber Command
IOC	Initial Operational Capability
MARFORCYBER	Marine Corps Forces Cyberspace Command
NMT	National Mission Team
NSA	National Security Agency
NST	National Support Team
TASKORD	Task Order
USCYBERCOM	U.S. Cyber Command

Whistleblower Protection

U.S. DEPARTMENT OF DEFENSE

The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD Hotline Director. For more information on your rights and remedies against retaliation, visit www.dodig.mil/programs/whistleblower.

For more information about DoD IG reports or activities, please contact us:

Congressional Liaison

congressional@dodig.mil; 703.604.8324

Media Contact

public.affairs@dodig.mil; 703.604.8324

Monthly Update

dodigconnect-request@listserve.com

Reports Mailing List

dodig_report@listserve.com

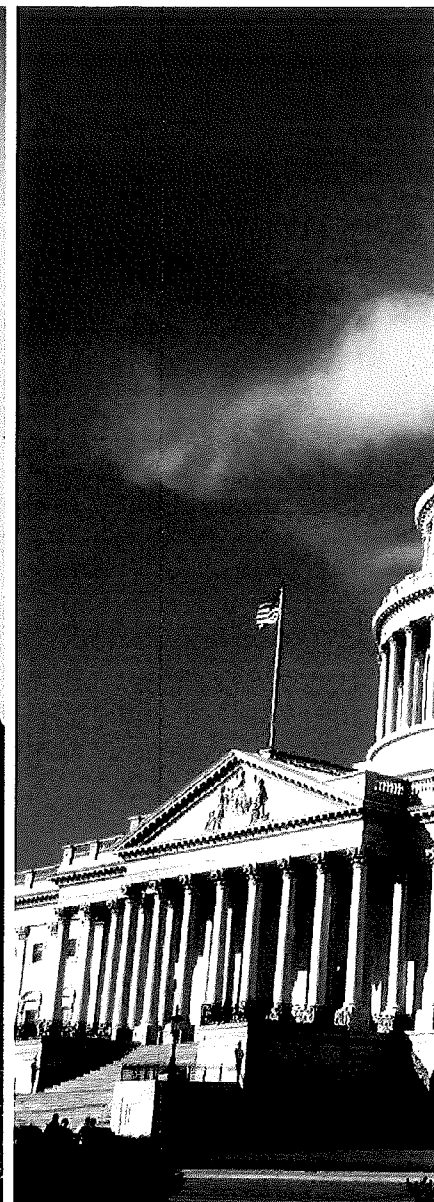
Twitter

twitter.com/DoD_IG

DoD Hotline

dodig.mil/hotline

SECRET//NOFORN



DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500

www.dodig.mil

Defense Hotline 1.800.424.9098

SECRET//NOFORN